PROGRAMME DE FORMATION

Adopter les bonnes pratiques en matière de cybersécurité

Les cyberattaques sont de plus en plus sophistiquées, mettant en danger les données et la réputation des organisations.
Dans 9 cas sur 10, les attaques aboutissent suite à une erreur humaine.
Tous les types de société sont concernés : de la TPE/PME aux Ministères.
1 attaque sur 2 aboutie avec succès, avec 3 grands types d'attaque : logiciel malveillant, phishing et rançongiciel.
Les salariés sont souvent la porte d'entrée des cybermenaces, cependant, **ils peuvent être la première ligne de défense**. Il en est de même pour vous Dirigeant, c'est pourquoi il est crucial de vous former en

- Apprenant à reconnaître les signes d'une attaque
- Adoptant les bonnes pratiques en matière de sécurité

OBJECTIFS PEDAGOGIQUES

✓ Être capable de comprendre la typologie des risques liés à la sécurité SI et les conséquences possibles
✓ Être capable d'identifier les mesures de protection de l'information et de sécurisation de leur poste de travail

PUBLIC CONCERNÉ :
Tout public

PRÉ-REQUIS :
Maîtrise des savoirs de base français

DURÉE EN PRÉSENTIEL :
1 jour soit 7 heures (par demi-journée)

DATES :
A définir

HORAIRES :
9h – 12h30

COÛT DE LA FORMATION :
700 € net de taxes / personne

DÉLAI D'ACCES :
Inscription minimum 15 jours avant le début de la formation

EFFECTIF GROUPE :
10 participants

LIEU :
21/23 rue de Courcelles 51100 REIMS

Parking payant dans la rue

LIEU - ACCESSIBILITE : ascenseur

Si besoin d'adapter notre formation, merci de prendre contact avec nous en amont
ecole.des.pme@cpme51.fr

CONTENU DE LA FORMATION :

- **Introduction à la cybersécurité**
  - Quelques chiffres pour contextualiser
  - Que dit le droit ?
- **Gestion des mots de passe**
  - Introduction : utilité des mots de passe
  - Les alternatives aux mots de passe
  - Adopter une stratégie de gestion de mots de passe
  - Quels sont les outils qui facilitent le quotidien ?
- **Se protéger contre les attaques de type phishing**
  - Comment reconnaître un e-mail frauduleux ?
  - Que faire en cas de doute ?
  - Les recommandations de l'ANSSI

PROGRAMME DE FORMATION

MOYENS ET METHODES PEDAGOGIQUES

Apports théoriques et pédagogie participative

SUPPORT REMIS

Mise à disposition au format PDF des supports de formation

Remise de fiches synthétiques

MOYENS PERMETTANT D'APPRÉCIER LES RÉSULTATS DE L'ACTION :

Durant la formation :

Mise en situation – QCM – questions orales

A fin de la formation :

Évaluation à chaud de la formation

Après la formation :

Envoi d'un questionnaire d'auto-évaluation à froid au stagiaire pour évaluer le transfert des acquis formation

Envoi d'un questionnaire à froid Entreprise pour évaluer le transfert des acquis en formation du ou des stagiaires

SANCTION DE LA FORMATION

Un certificat de réalisation sera transmis à chaque stagiaire

PROFIL INTERVENANT :

Organisme certifié QUALIOPI

Intervenant expert avec plus de 25 ans dans le domaine informatique
Une expérience de 10 ans dans le domaine de la formation sur des thématiques cyber
Accompagnateur d'Entreprises sur les sujets cyber
A dispensé cette formation à des publics variés : de maisons de Champagne en passant par le GIGN. La formation s'adapte aux besoins et au contexte de l'entreprise.

LES + :

Si vous souhaitez réaliser cette formation en INTRA, dans votre

Entreprise, voici ce que nous vous proposons :

- Une **rencontre préalable** avec le Dirigeant/Responsable pour l'écoute des besoins et un **audit de sécurité sur site**
- Avec son accord, une **tentative d'intrusion simple** (via mail par exemple) pour analyse des réactions équipes en amont de la formation
- Présentation des **résultats de cette attaque** + **Formation sur mesure**
- A distance de la Formation, une **nouvelle tentative d'attaque** pour analyse des réactions post Formation

- Un suivi de **3 mois post Formation** pour étude des comportements, et analyse des failles survenues et mises en pratique

L'expertise de notre intervenant nous permet de co-construire des modules de formation adaptés à vos besoins spécifiques :

. DevSecOps : formation de vos équipes aux meilleurs pratiques de sécurité dans le développement et le DevOps

. Sécurité des infrastructures : icloud ou infrastructures on-premise

. Formations dédiées à la lutte contre la fraude : e-commerce – paiements en ligne – KYC …

Contactez-nous si intéressé(e)s et nous vous transmettrons une offre sur mesure